Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 73 (2015) 282 – 289

Procedia Computer Science

The International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015)

Trust-based Scheme for Alert Spreading in VANET

Amel Ltifi [a], Ahmed Zouinkhi [b], Mohamed Salim Bouhlel [a]

a Research Unit: Sciences and Technologies of Image and Telecommunications, Higher Institute of Biotechnology of Sfax-Tunisia
b Research Unit: Modeling, Analysis and Control of Systems, National Engineering school of Gabes-Tunisia

Abstract

Currently, serious investigations are made now in road security as a critical research domain. However, the majority of them are based on expensive infrastructure. In this paper, we propose a new scheme for warnings spreading between vehicles without any dependence on road foundation. A new concept of Active vehicle that combines the power of the intelligence ambient and the V2V technologies is introduced. For alert endorsement, we suggest a new model for trust management for VANET based on only the cooperation between "Active vehicles" in order to enhance their security states and to cut with the spread of false warnings through a vehicular network.

Peer-review under responsibility of organizing committee of the International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015)

Keywords: ambient intelligence; security; cooperation; active vehicle; trust management; VANET;

1. Introduction

Road safety is the purpose of many researches and projects over the world, given the huge number of deaths and accidents [1]. VANET is a set of vehicles. Each vehicle can communicate with other vehicles using DSRC (Dedicated Short Range Communication) technology (5.9 GHz) that supports ranges of up to 1 KM [2]. Currently, VANET is the principal element in most current suggestions aimed to enhance driving conditions. Intelligence ambient and ubiquitous computing are new challenging technologies that can be used among VANET applications [3]. Many technical disputes are addressed by the researchers for the dissemination and large use of VANETs. These disputes are tackled by several projects. FleetNet is one of these projects [4]. Its main aim is to build up applications for V2V communication. Network on Wheels (NoW) [5] and CarTALK2000 [6] are others outstanding projects for road safety. Car-to-Car Communication Consortium (C2C-CC) [7] is an industry Consortium supervising VANET research domain in Europe. It attempts to develop standards for vehicle to vehicle and vehicle to infrastructure communications [8]. Immense studies have also been done on the improvement of road safety mechanism [9], such

Peer-review under responsibility of organizing committee of the International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015)
doi:10.1016/j.procs.2015.12.031

as collision avoidance [10], alert message spreading [11] and traffic management [12]. Therefore, many suggestions are found for the reliability of messages. However, few studies are addressing the evaluation of trustworthiness of transmitted warning messages between vehicles.

Researchers in [13], [14] and [15] suggested some possible solutions for trust management used in MANET. These methods use historical records or reputation data for trust management. Therefore, applying MANET's traditional solutions is not suitable for VANET in the absence of stored past information. Nowadays, many research projects like NoW [5] and Safespot [16] are interested in the intuitive communication between vehicles (V2V) or between vehicles and roadside infrastructure (V2R).

Throughout this work, we have implemented a new communication protocol between vehicles. The main aim of this protocol is to attribute to each vehicle on the road a trust value reflecting its behavior and its contribution in the spread of critical information among peers. This trust value is used to evaluate the trustworthiness of transmitted warning messages in dangerous states. Therefore, a trust model is created and updated throughout vehicles communication. Each vehicle has a role in the trust management system. The group leader is a particular vehicle. It performs some tasks of the trusted authority by managing trust values of the group members and by verifying the validity of alarm messages transmitted in the group. The aim of this protocol is to help vehicles to make the right decision about the trustworthiness of received alert messages.

The rest of the paper is organized as follow: First, the second section introduces the model design of the suggested scheme and it describes each component of the solution. We dedicated the third part for model evaluation. Finally, a brief summary of the work is included in the conclusion.

2. Component-based architecture for the system

The proposed Self-Organized Trust Management system contains four principal modules as depicted in figure 1. In this section, we will explain the roles of these four modules and the interaction between them.

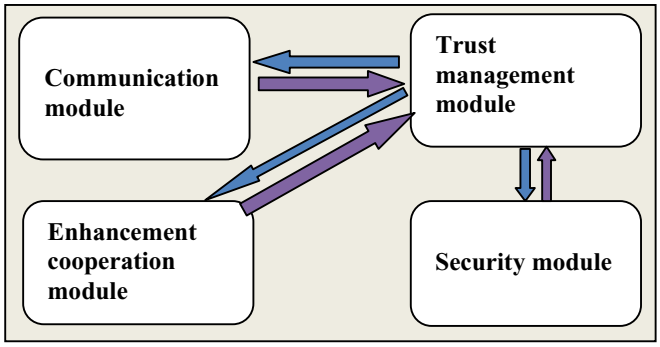

Fig. 1 Model design

2.1. Communication module

When a VANET application uses only the communication mode V2V, there is zero dependence to the infrastructure. There is no need to the Road-Side-Units (RSUs) or any other outside infrastructure. This kind of application is very close to ad-hoc networks. In this situation, vehicles manage themselves the traffic state. The V2V uses for network connection the standard IEEE 802.11p specification [17]. The 802.11p is an approved variant of the standard 802.11 used for Wi-Fi. The used band of spectrum is between 5.85GHz and 5.925GHz.

Figure 2 illustrates the vehicles organization on the road. For each community of vehicles, there is a group leader that has the role of a trusted authority as depicted in figure 2. There are two types of links between vehicles: Unicast link and broadcast link.

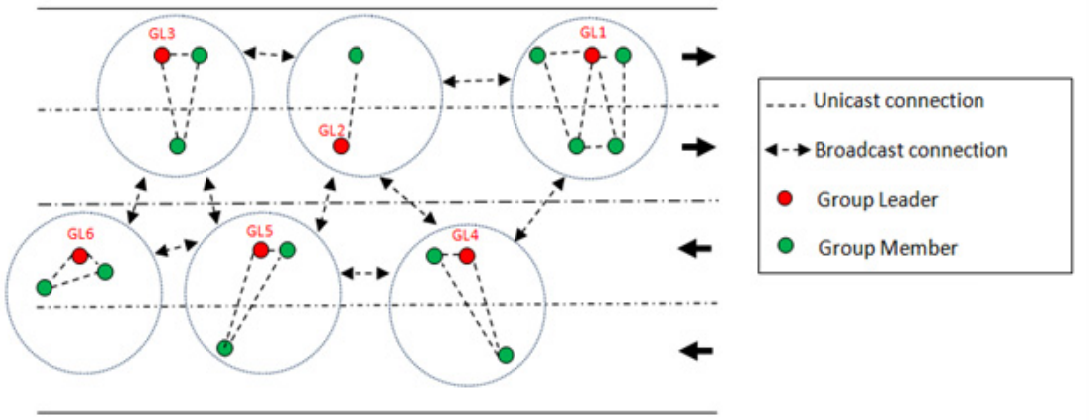

Fig. 2 Connection model between vehicles

The vehicle-to-vehicle communication can be used alone on account of the existence of new wireless technologies and especially the IEEE 802.11p standard. The inter-vehicular communication gains benefit from wireless ad-hoc Networks and GPS to guarantee stable one hop and multi hop communications between vehicles [18].

The inter-vehicle communication model employs the IEEE 802.11p standard as well as a set of advanced management and routing algorithms. The V2V applications include the intelligent movement assistance, the emergency state management and the route access. The intelligent traffic management algorithms intend to minimize the number of road accidents and the traffic congestion. The V2V technique allows vehicles to exchange messages by operating the store-carry-and-forward approach [19] where a node can store a received message and transmitted it to another node when a connection is established.

Routing algorithm is the mainly challenging mission for VANET because of the strict requirements of VANET to high speed mobility and a rapidly changing topology [20]. For these reason, we opted to use a clustered architecture to create a network vision more stable and more reduced for each vehicle [21].

The clustering is well suited to VANETs since the vehicular traffic dynamics causes a spontaneous creation of a number of geographical clusters. By dividing the space, the network can be easier to manage and the control messages are not necessary exchanged between all the vehicles but only between vehicles in the same group. The embedded technologies in the intelligent vehicles allow improving the precision of the vehicle position thanks to the global map position, the embedded sensors as the radars and the odometer. Multiple suggestions of clustering are using these technologies of localization.

2.2. Trust management module

Recently, VANET makes the interest in Ambient Intelligence (AmI) Environments grown considerably given the contribution of such environment in the improvement of the active security. We have introduced in our study the concept of “Active vehicle” that illustrates the integration of two highly innovative technologies: AmI and VANET. Active vehicle is an ambient intelligent vehicle. This vehicle is well equipped to achieve many tasks in the same time. An active vehicle can cooperate with other vehicles, it can transmit and acquire data and it decides and reacts to the disturbances of its environment. Therefore, these capabilities allow the vehicle to affect, to cooperate, to transform the behavior of its environment. Hence, the vehicle is a proactive actor on the road. Based on wireless communication, its embedded sensors and its ambient capabilities, it manages itself its security state regardless of any infrastructure.

The security state management of vehicles is the aim of our trust management module. Based on a clustering approach, an intelligent vehicle, in our context, can play two different roles: a group member or a group leader.

2.3. Enhancement cooperation module

Our enhancement cooperation approach is inspired by "Neighborhood WatchDog" [22] solution. In the proposed cluster-based trust management system, the GL plays the role of the watchdog. It detects the misbehaved vehicles and it eliminates them from the group when it is necessary. It has a list of all vehicles members in the group. Each entry in the list contains the Id of a vehicle, its address, its TV value and its CC value. These two counters are updated according to the vehicle acting way in warnings transmission sessions.

a. Exchanged messages

Active vehicles exchange a list of messages between them in order to manage their security state in the absence of a trusted authority. Due to the suggested model, only valid emergency messages are transmitted. Any other false warning is detected and the misbehaved vehicles are eliminated. The exchanged messages are:

- **The «HELLO» packet:** the first packet sent periodically on broadcast by a vehicle aimed to enter to the secured community until the receipt of the « AckHELLO » packet. This periodic control packet is used to maintain a continuous connectivity between the vehicle and the GL and between the vehicle and its successor.
- **The «AckHELLO» packet:** sent by the leader to a vehicle V as a response to the « HELLO » packet. The vehicle V registers the address of the leader to be used in the communication.
- **The "theSUCC" packet:** is the response to the "HELLO" packet sent by a vehicle V when it is received by the successor of V.
- **The « GRE » packet :** sent periodically by each vehicle to the leader after receiving an « AckHELLO » from the leader;
- **The «WARNING» packet:** contains some information on an alarm event, it is sent by the vehicle that detects the alarm state to the leader to be verified and registered.
- **The "IsTRANSMITTED" packet**: sent to the leader by a vehicle after transmitting the alarm packet to another vehicle. It contains the Id of the source, the Id of the destination, the Id of the warning packet and the transmission time of the alarm packet. The Id of the warning packet is a unique identifier assigned to each launched warning to distinguish between different warning transmission sessions.
- **The «AckWARNING» packet:** sent by the leader to the vehicle that has detected the alert state. It designs that the leader accepts the warning message received after verifying the trust model registered on its database.
- **The «ALARM» packet:** it contains a hashed and encrypted warning data, exchanged between intermediated neighbors.
- **The «ALARMFromBROADCAST» packet:** it contains the warning message, sent on broadcast by the leader and by each intermediate vehicle receiving an "ALARM" packet. The trustworthiness of this packet is not guaranteed. But, it aims to increase the number of vehicles receiving the warning message.
- **The «CONFIRM» packet:** sent to the leader by each vehicle after receiving an « ALARM » packet in order to verify its validity.
- **The «VALIDATION» packet:** sent by the leader as a response to the « CONFIRM » packet. It means that the leader confirms the validity of the « ALARM » packet.
- **The «CorrVALIDATION» packet:** After receipt of the "CONFIRM" packet and when the leader discovers that the « ALARM » packet has been changed, then the leader would send the original alarm data that are stored in its buffer to prevent spread of erroneous messages**.**
- **The «ERROR» packet:** sent by the leader to a vehicle to stop the spread of the « ALARM » packet.

b. Warning transmission session

The warning transmission session begins when a vehicle S detects an obstacle or an accident and it decides to inform other vehicles about it. Therefore, the vehicle S sends a WARNING message to the GL that verifies its validity according the TV of the vehicle S. When it is validated by the GL, the vehicle S sends an ALARM message to its successor. The successor sends a CONFIRM message to the GL to validate or not the information received in the ALARM message. In the validation case, the ALARM message is transmitted to the vehicle V_{i+1} the successor of the vehicle V_i. Figure 3 shows the exchanged messages in a normal transmission session where all contributor vehicles are well-behaved. Where there is an abnormal behavior, many scenarios are possible. In this case, the warning transmission session is interrupted by the GL.

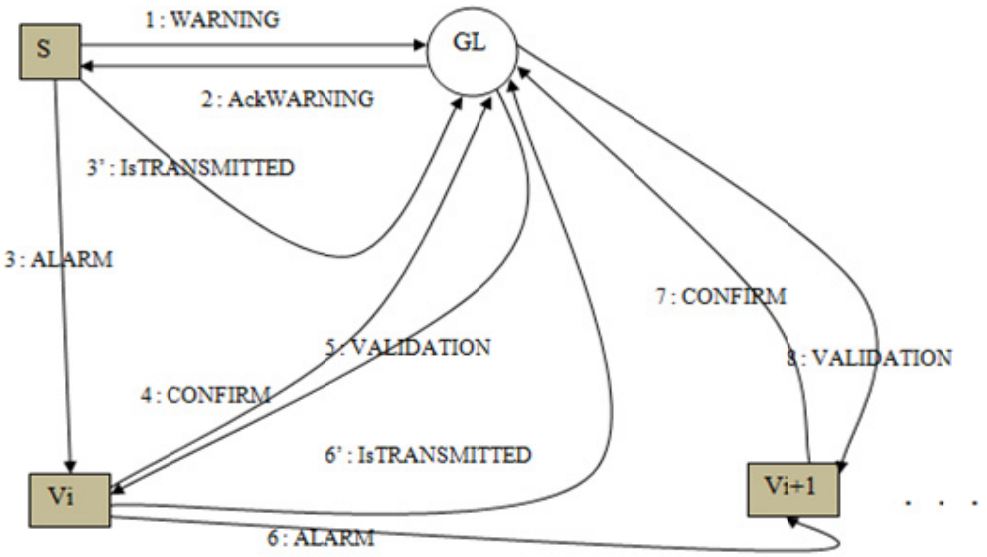

Fig. 3 Alarm transmission session

2.4. Security module

Currently, Wireless technology introduces many possible risks to users because of its huge spread. The security module, in our model, provides a solution for these possible risks. We inspired our security solution from the PGP (Pretty Good Privacy) algorithm that is used hugely in a self-organized network as VANET [23]. Social relationships between vehicles are close to those in the PGP system [24]. Unless, the very large amount of source of the complete PGP version makes from its comprehension and use a difficult task [25]. For this reason, we focused only to use the cryptographic and the hash methods used by PGP which are RSA and SHA. Our security module implies the algorithm SHA1-RSA [26]. RSA [26] is a public-key cryptosystem for both encryption and authentication. The public-key cryptography has many advantages [27] as providing the possibility to implement digital signatures. Many existing solutions for VANET security are using RSA [26], [28-30]. We applied the SHA-1 [31] function with the RSA encryption method. RSA is combined with the SHA1 hashing function to sign a message in this signature suite.

The group leader is in charge of the key distribution in its group. Each vehicle has a pair of public/private key generated by its OBU (On Board Unit). In the announcement step, each vehicle sends its public key to the leader to be used later in the communication step. When a vehicle A receives an ALARM message from its predecessor B, B sends a CONFIRM message to the leader to verify the trustworthiness of the message and to obtain the public key of A in order to verify the sender authenticity by comparing the signature sent with the ALARM message and the computed one. Figure 4 illustrated on details all the steps followed by the sender and the receiver of an ALARM message.

3. Evaluation

In road safety, a good trust management system has short delay, according to the necessity of a real time and effective decision making. Therefore, we will show and discuss in this section some results obtained by simulation of different scenarios in order to verify the efficiency of the proposed approach. We will study the results from two aspects: the number of vehicles employing our protocol and the average end-to-end delay of messages. Values of simulation parameters used are shown in table 1.

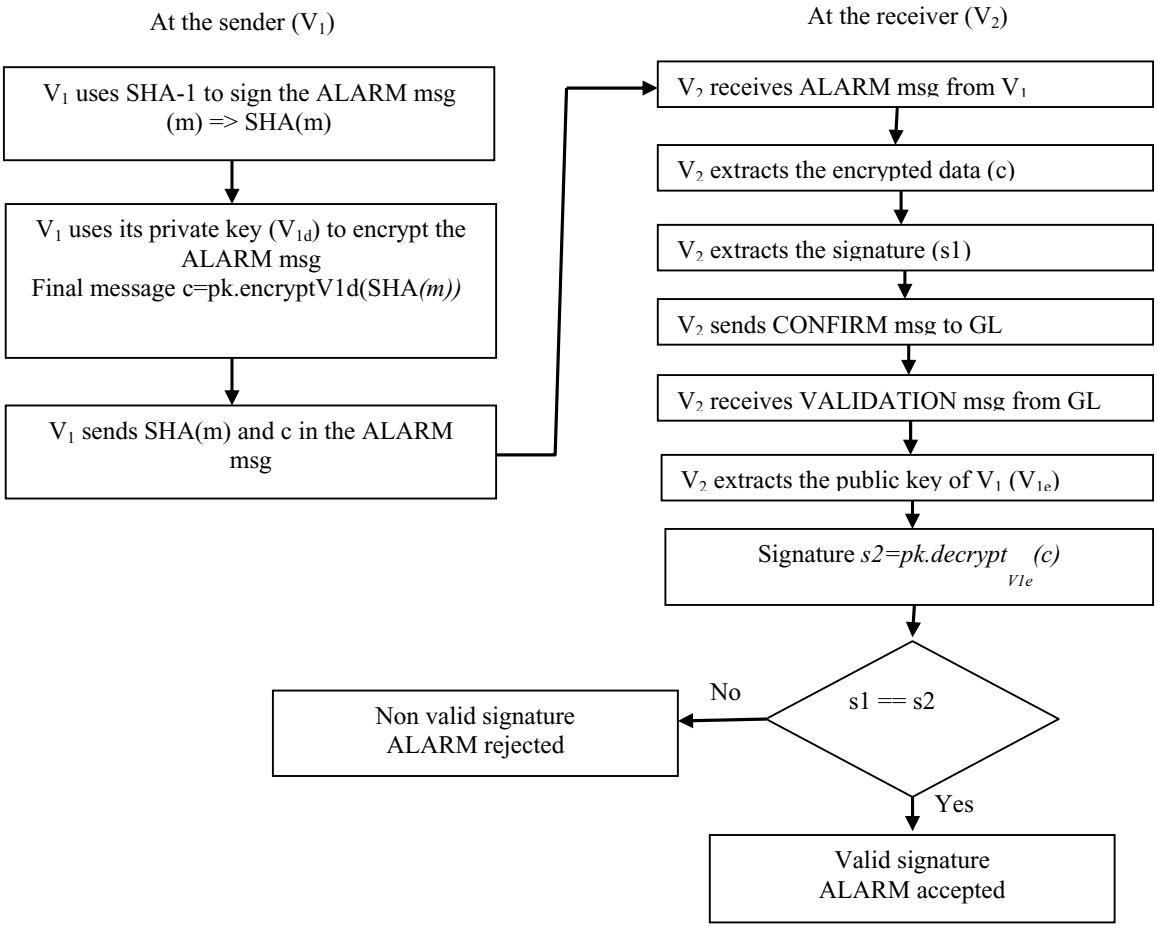

Fig. 4 Authentication and signature verification

We used the statistics module provided by the NS-3 simulator to generate the graph illustrated by figure 5 for an average delay. The end-to-end delay calculated by the statistics module, provided by the NS-3 simulator, is the difference between the reception time of a packet and its sending time between two nodes. In order to illustrate the impact of vehicles speed in the end-to-end delay and evaluate our obtained results, figure 5 contains three graphs for three different speeds (29 km/h, 60 km/h and 90 km/h), which were compared to results obtained by an infrastructure based authentication approach for VANET described in [32]. The simulation results proved that the network overhead introduced by our suggestion for three different speeds is well under the overhead introduced by the approach presented in [32] that ensures only a part of functionalities provided by our model. The majority of existing strategies for road safety are based on road infrastructure even new suggestions [33]. The comparison with [32] aims to move new strategies toward to self-organized trust management systems giving the huge difference between end-to-end delays in based infrastructure approach and non based infrastructure approach.

According to figure 5, the overhead introduced by our protocol is under the threshold fixed by the DSRC [34] that is 100 ms, although, this overhead is caused by messages sent periodically to maintain the linkability between vehicles (ex. the GRE packet). And, it can be reduced by studying and measuring the impact of the periodic time of such a control packet on the network delay in order to obtain the lowest overhead.

Table 1Simulation parameters

Simulation parameter	Value
Speed Limit of Vehicles	29 Km/s, 60 Km/s, 90 Km/s
Acceleration/deceleration	0.5ms-1/3ms-1
Number of vehicles	8 to 40
Transmission power	21db
Simulation time	19s to 80s
Communication protocol	802.11a
Data rate	6Mb/s

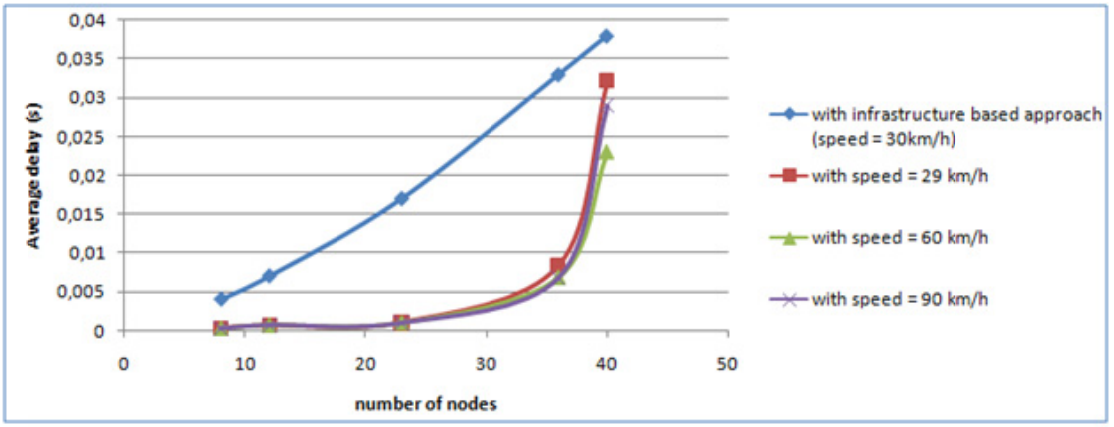

Fig. 5Average Delay generated between 2 nodes: V0 and V2

4. Conclusion

We proposed in this paper a new scheme for warnings transmission between vehicles in a secure way. Nevertheless, our solution is totally based on vehicles cooperation. The proposed model deals with the cooperation enhancement issue as a principal component in our approach. Compared to other solutions suggested for VANET, the new approach pledges in the same time first the transmission of only the true ALARM messages and second the registration/updating of vehicles trust values based on historical and runtime vehicles behaviors. Finally, according to simulation results, we found that the end-to-end delay of the system is well under the tolerant delay constraint defined by the DSRC. Although, the privacy issue that is not yet addressed by our solution, will be a priority task in future works.

References

1. Samara G, Al-Salihy WAH, and Sures R. Security issues and challenges of vehicular ad hoc networks (VANET), in Proceedings of the 4th International Conference on New Trends in Information Science and Service Science (NISS '10), Gyeongju-si, Republic of Korea, May 2010; 393–398.
2. Taha MMI, Hasan YMY. VANET-DSRC protocol for reliable broadcasting of life safety messages. In Proceedings of the IEEE International Symposium on Signal Processing and Information Technology (ISSPIT '07); 2007; 104–109.
3. Gillani S, Khan I, Qureshi S, Qayyum A. Vehicular ad hoc network (VANET): enabling secure and efficient transportation system. Technical Journal, University of Engineering and Technology, Taxila; vol. 13; 2008
4. Franz W, Wagner C, Maihofer C, Hartenstein H. Fleetnet: Platform for inter-vehicle communications. In Proceeding 1st International Workshop on Intelligent Transportation, Hamburg, Germany; 2004.
5. Abusch-Magder D, Bosch P., Klein T-E, Polakos P-A, Samuel L-G, Harish V. NOW: A Network on Wheels for Emergency Response and Disaster Recovery Operations. Bell Labs Technical Journal ; 2007; 11(4); 113–133.

6. D. Reichardt, Miglietta, M. Moretti, L. Morsink, P. Schulz,W. CarTALK 2000: Safe and Comfortable Driving Based uponInter Vehicle Communication. Intelligent Vehicle Symposium,2002. IEEE, vol. 2; 2003; 545-550.
7. Car 2 Car Communication Consortium Manifesto. version 1.1, technical report , Aug 2007 Available: www.car-to-car.org
8. Jerbi M, Senouci SM, Cherif M, Ghamri Y. Vehicular Communications Networks: Current Trends and Challenges. Book Chapter in Next Generation Mobile Networks and Ubiquitous Computing, IGI Global; 2010.
9. Zhang, J.: A Survey on Trust Management for VANETs. International Conference on Advanced Information Networking and Applications, Biopolis, Singapore; 2011; 105–112.
10. Nadeem T, Dashtinezhad S, Liao C, Iftode L. Trafficview: Traffic data dissemination using car-to-car communication. ACM SIGMOBILE Mobile Computing and Communications Review; 2004.
11. Xu Q, Mak T, Ko J, Sengupta R. Vehicle-to-vehicle safety messaging in DSRC. in Proceedings of VANET; 2004.
12. Elbatt T, Goel SK, Holland G, Krishnan H, Parikh J. Cooperative collision warning using dedicated short range wireless communications. In Proceedings of VANET; 2006.
13. Cho J-H, Swami V. Towards trust-based cognitive networks: A survey of trust management for mobile ad hoc networks. In: Proceedings of the 14th International Command and Control Research and Technology Symposium, Washington, DC; 2009.
14. Cho JH, Swami A, Chen IR. A survey on trust management for mobile ad hoc networks. IEEE Communications Surveys and Tutorials 2011; 13(4); 562-583.
15. Balakrishnan V, Varadharajan V, Tupakula U. Trust management in mobile ad hoc networks. In Handbook of Wireless Ad hoc and Sensor Networks, Springer; 2009, 473–502.
16. Manzoni V, Codecà F, Savaresi S, Cravini P. The Implementation of the Safespot Architecture on a Powered Two-Wheeler Vehicle. 12th IFAC Symposium on Control in Transportation Systems (CTS 2009), Redondo Beach, CA, USA, September 2009; 450-455.
17. Jagdeep Kaur, Er.Parminder Singh,"Performance Comparison Between Unicast And Multicast Protocols In Vanets", International Journal Of Ad- vanced Technology & Engineering Research; 3(1); 2013;109-115.
18. Malla AM, Sahu RK. A Review on Vehicle to Vehicle Communication Protocols in VANETs. IJARCSSE; 3(2); 2013.
19. Shukla RS, Khan IA, Tyagi N. Performance of Modified Edge Based Greedy Routing Algorithm in VANET Using Real City Scenario. Advances in Mechanical Engineering and its , Applications (AMEA); 2(3); 2012.
20. Yu JY, Chong PHJ. A Survey of Clustering Schemes for Mobile Ad Hoc Networks. IEEE Communications Surveys and Tutorials; 7(1); 2005;32–48.
21. Ltifi A, Zouinkhi A, Bouhlel MS. A Trust Management System Through Ambient Communication For Vanet. International Journal of Informatics and Communication Technology (IJ-ICT); 2(2); 2013;71-78.
22. Hortelano J, Ruiz J-C, Manzoni P. Evaluating the Uselfusness of Watchdogs for Intrusion Detection in VANETs. IEEE International Conference on Communications; 2010.
23. Randhawa, Navdeep Kaur. "Design and Implementing PGP Algorithm in Vehicular Adhoc Networks (VANETs)," International Journal of Engineering Research and Applications, Vol. 2, Issue 3, May-Jun 2012, pp. 647-650
24. Shafiullah Khan and Al-Sakib Khan Pathan, "Wireless Networks and Security: Issues, Challenges and Research Trends", Springer Series: Signals and Communication Technology, 2013, pp. 107-132, ISBN 978-3-642-36168-5
25. Kurniawan, Y., Albone, A., & Rahyuwibowo, H. The design of mini PGP security. International Conference on the Electrical Engineering and Informatics (ICEEI), Indonesia, 17-19 July, 2011.
26. Sophia A-J. A Score Based Trustworthy Declaration Scheme For Vanets, International Journal of Engineering Research and Applications, 2014; 4(3); 542-544.
27. Rivest R, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 1978; 21(2): 120–126.
28. Serna J., Luna J. Medina M. Geolocation-based Trust for Vanet's Privacy. Journal of Information Assurance and Security 2009; 4(5):432-439.
29.Alangudi B-N, Mahalakshmi R-S. Privacy Preserving Authentication for Security in VANET. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 2014; 2(1): 200-203.
30. Verma M, Dijiang H. SeGCom: secure group communication in VANETs. In Proceedings of 6th IEEE consumer communications and networking conference (CCNC 2009), Las Vegas, January 2009.
31. Zhang J-P, Chen C, and Cohen R. Trust based decision making on message relay and local actions in VANET. Journal of Security Communication Networks, 2013; 6(1): 1-14.
32. Chaurasia B-K, Verma S. Infrastructure based Authentication in VANETs. International Journal of Multimedia and Ubiquitous Engineering 2011; 6(2): 41-54.
33. Engoulou R. G., Bellaïche M., Pierre S., Quintero A. VANET security surveys, International Journal of Computer Communications 2014 ; 40:1–13
34. Anwer MS, Guy C. A Survey of VANET Technologies. Journal of Emerging Trends in Computing and Information Sciences. 5(9); 2014; 661-671.